REMARKS

Claims 1-50 are pending, of which Claims 1, 26, 49 and 50 are independent. Claims 1-50 were rejected under 35 U.S.C. §102(b), and Claims 18 and 50 are subject to objections. For the reasons discussed below, all claims are in condition for allowance.

Regarding Claim Objections

Claims 18 and 50 were objected to because of informalities. In response, Claims 18 and 50 are amended. Reconsideration of the objections is respectfully requested.

Regarding 35 U.S.C. §102(b) Claim Rejections

Claims 1-50 were rejected under 35 U.S.C. §102(b) based on U.S. Patent No. 6,170,060 to Mott et al. These rejections are traversed.

Disclosed embodiments of the invention relate to an approach for identifying software using a superfingerprint. Specified portions of at least one of said executing software and of results of executing said software are selected. Computations are performed on the selected potions to create a collection of fingerprints. The collection of fingerprints is combined according to a combining rule to create a superfingerprint of the executing software. The superfingerprint can be used to identify the software, and determine, for instance, whether anyone has tampered with the software.

If, for example, the executing software is a Java bytecode stream that is being executed by a Java Virtual Machine, a superfingerprint can be created by processing and performing computations on portions of the bytecode stream. For instance, portions of the bytecode stream can be selected and computations can be performed on the selected portions to obtain a collection of fingerprints. A fingerprint, for example, can be a hash function value of a sequence of instructions, such as operand codes in the bytecode stream. The fingerprints can be collected and combined according to a combining rule to create a superfingerprint. When the software is executed again, portions of the executing software can be compared with their corresponding fingerprints to identify the software and determine whether it has been altered.

A. Mott's Software Identification Approach Does Not Relate to the Claimed Superfingerprint

Although Mott relates to an approach that ensures that software, such as downloaded software, has not been altered, Mott's technique does not use the claimed superfingerprints. Mott relates to a media playback approach that allows downloaded content to be played on the playback device if the downloaded content has been digitally signed and the downloaded content and the playback device have matching IDs. In particular, Mott's authentication approach relies on comparing the playback device's player ID with an embedded ID in the downloaded content, and on verifying a digital signature appended to the downloaded content. Specifically, according to Mott, the downloaded content is formatted so that when it is downloaded, it can only be played by a player device that has a player ID that matches the embedded ID in the downloaded content. In addition, a digital signature is appended to the downloaded content for use by the playback device to confirm that that the downloaded content originates from an authorized server.

While Mott's approach relies on player IDs, content IDs, or digital signatures to identify digital content, the claimed approach creates superfingerprints to identify executing software by selecting portions of executing software, performing computations on the portions, creating fingerprints from the computations, and combining the fingerprints to create a superfingerprint. As such, Mott does not relate to the claimed superfingerprint.

B. Mott's Software Identification Approach Does Not Identify Software By Executing the Software

The claimed software identification technique performs computations on selected portions of the *executing software* to compute fingerprints that are combined to create a superfingerprint. The superfingerprint is used to identify the executing protected software. By way of contrast, Mott does not execute the protected software to identify it. Instead, Mott uses an appended digital signature in the downloaded software and embedded IDs in the downloaded software and playback device to identify and authenticate the downloaded software. Although Mott eventually executes software once it has been identified, Mott does not use any information from the execution of the software to perform the software identification. Thus, unlike the

claimed invention, Mott's software identification scheme is not directed to an approach that executes the protected software in order to identify it.

Moreover, Mott's software identification approach only identifies and verifies software that originates from an authorized source. According to Mott, not only does the software need to be digitally signed for it to execute using the player device, but it also needs to be created with Mott's particular "authoring system." In this way, Mott's software identification approach will not identify software created using a different authoring system. Indeed, Mott's software identification approach is very limited, and it does not address the problems associated with identifying software that has been developed using an approach other than Mott's particular authoring scheme. Specifically, unlike Mott, the claimed technique for identification can detect software pirated from legitimate vendors, stripped of names, digital signatures, and other identifying appendages.

By way of contrast, the inventive software identification technique does not require that the software that is being identified be from "an authorized source." In fact, the software being identified could come from any source, and it could be any type of software. The claimed approach can identify any type of software from any source by creating a superfingerprint of executing portions of the software. Thus, unlike Mott, the claimed technique provides a software identification scheme that can identify software independent of the authoring environment or source of the software.

C. The Office Has Not Made A Prima Facie Case of Anticipation Under §102 Based on Mott

For the reasons discussed above, the Office has not made a prima facie case under §102 because Mott does not discuss every limitation of the claimed invention, namely:

- in each execution, selecting specified portions of at least one of said executing software and of results of executing said software;
- in each execution, performing computations on said selected portions to obtain a collection of fingerprints; and

- combining said collections of fingerprints found in each execution into the superfingerprint of said software according to a combining rule, as set forth in Claim 1 and similarly set forth in Claims 26, 49 and 50.

Therefore, it is respectfully requested that the rejections of Claims 1, 26, 49 and 50 and their respective dependent claims under § 102 based on Mott be reconsidered and withdrawn.

Information Disclosure Statement

An Information Disclosure Statement (IDS) is being filed concurrently herewith. Entry of the IDS is respectfully requested.

CONCLUSION

In view of the above amendments and remarks, it is believed that all claims are in condition for allowance, and it is respectfully requested that the application be passed to issue. If the Examiner feels that a telephone conference would expedite prosecution of this case, the Examiner is invited to call the undersigned attorney.

Respectfully submitted,

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

By _____

James M. Smith
Registration No. 28,043
Telephone: (978) 341-0036
Facsimile: (978) 341-0136

Concord, MA 01742-9133
Dated: 1/20/6